UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,815	10/11/2001	Neal A. Krawetz	10019968-1	9182

7590 06/12/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/975,815	KRAWETZ, NEAL A.	
	Examiner	Art Unit	
	CARL COLIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 2/19/2008, applicant amends claims 1, 11, 19, and 27. The following claims 1-34 are presented for examination.

1.1 Applicant's remarks, pages 8-10, filed on 2/19/2008, with respect to the rejection of claims 1-34 have been fully considered but they are not persuasive as amended. Applicant argues that Bowman appears to disclose using the same key for encryption. Examiner respectfully disagrees as Bowman discloses a key generated from random string to make the encrypted data less susceptible to cryptanalysis (see column 4, lines 39-45) and also discloses secret ID to select corresponding secret key (see column 9, lines 27-29); therefore, it would have been obvious to one of ordinary skill in the art to use different key to make the encrypted data less susceptible to cryptanalysis. Upon further consideration a new ground of rejection is made in view of Bowman and Roberts. Roberts discloses a hash key used for encryption that is different for each data packet associated with a secure data transmission.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The cited portion indicated by applicant page 8, lines 25-27, citing "*unlike secure shell and other tunneling protocols the encryption key changes with each transmitted data packet*" , which is the only section of the disclosure mentioning encryption key change and data packet, is not equivalent to the added limitations of the claims as amended. Applicant amends claim 1 to recite "generated a character string at a sender for each data packet associated with the secure data transmission"; "generating a hash key wherein the hash key is different for each data packet associated with the secure data transmission"... "encrypting a data packet associated with the secure data transmission". Applicant's specification page 8, lines 25-27 fails to provide support for these limitations in the claim. For instance, there is no description in the disclosure for specifying which part of the encryption key changes for each data packet and there is no disclosure of data packet associated with the secure data transmission. Therefore, independent claims 1 and 19 are not supported by the original specification as amended. Claims 11 and 27 have been amended to recite "receiving plurality of character strings... receiving plurality of encrypted data packets each of the plurality of character strings correspond to one of the plurality of encrypted data packets... decrypting the plurality of encrypted data packets and the respective character strings. Neither one of these limitations is supported by the original specification as amended.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4, 5, 7, 8, 11, 12, 14, 15, 19, and 22-25 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,931,128 to **Roberts**.

As per claim 1, Roberts discloses a method for secure data transmission, comprising: generating a character string (seed) at a sender for each data packet associated with the secure data transmission (see column 3, lines 21-27);
generating a hash key using the character string (seed) and a private key (master secret) (see column 7, lines 34-67); wherein the hash key is different for each data packet associated with the secure data transmission (see column 10, lines 38-42) encrypting a data packet associated with the secure data transmission using the hash key (see column 9, lines 55-67); and transmitting an identification key (SPI) associated with the sender, the character string (seed), and the encrypted

data packet from the sender to a recipient (see column 6, lines 45-54 and column 9, line 62 through column 10, line 5).

As per claim 2, Roberts discloses the limitation of wherein generating the hash key comprises hashing the character string (seed) with the private key (master secret) (see column 7, lines 34-67).

As per claim 4, Roberts discloses wherein generating a character string comprises randomly generating the character string (see column 7, lines 12-32).

As per claim 5, Roberts discloses determining the private key (master secret) at the recipient using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 58-67); and decrypting the encrypted data at the recipient using the private key (master secret) and the character string (seed) (see column 10, lines 13-31).

As per claim 7, Roberts discloses determining the private key (master secret) at the recipient using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 58-67); determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31); decrypting the encrypted data using the hash key (see column 10, lines 13-31).

As per claim 8, Roberts discloses wherein determining the hash key comprises hashing the character string (random seed) with the private key (master secret) (see column 7, lines 34-67 and column 10, lines 18-21, stating the same procedure is performed at the decryption device).

As per claim 11, Roberts teaches a method for secure data transmission, comprising:
receiving a plurality of character strings (random seed) from a sender (see column 10, lines 37-42);
receiving an identification key (SPI) from the sender (see column 6, lines 45-54 and column 9, line 62 through column 10, line 5);
receiving a plurality of encrypted data packets from the sender each of the plurality of character strings correspond to one of the plurality of encrypted data packets (see column 10, lines 37-48 and column 11, lines 3-29; and column 13, lines 13-26);
determining a private key (master secret) associated with the sender using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 62-67); and decrypting the plurality of encrypted data packets using the private key (master secret) and the respective character strings (random seed) (see column 11, lines 3-29 and column 13, lines 13-26).

As per claim 12, Roberts discloses determining a hash key using the private key (master secret) and the character string (random seed) (see column 13, lines 13-26); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see column 13, lines 13-26).

As per claim 14, Roberts discloses wherein receiving a character string (random string) comprises receiving a randomly generated character string (see column 7, lines 12-32).

As per claim 15, Roberts discloses hashing the character string (random seed) with the private key (master secret) to generate a hash key (see column 7, lines 34-67 and column 10, lines 18-21); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see column 10, lines 13-31).

As per claim 19, Roberts teaches a system for secure data transmission, (see fig. 1-2) comprising: a processor; a memory coupled to the processor (see fig.1); a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (see column 4, lines 8-23 and column 7, lines 12-31); a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string (random seed) and a private key (master secret) (see column 7, lines 32-67) wherein the hash key is different for each data packet associated with the secure data transmission (see column 10, lines 38-48); an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key (see column 9, lines 55-67) and wherein the processor is adapted to transmit the encrypted data, an identification key (SPI) related to the private key (master secret), and the character string (random seed) to a recipient (see column 6, lines 45-54 and column 9, line 62 through column 10, line 5).

As per claim 22, Roberts discloses wherein the hashing engine is adapted to hash the character string (seed) with the private key (master secret) to generate the hash key (see column 7, lines 34-67).

As per claim 23, Roberts discloses wherein the string generator is adapted to randomly generate the character string (random seed) (see column 7, lines 12-32).

As per claim 24, Roberts discloses wherein the recipient is adapted to decrypt the encrypted data using the identification key (SPI) and the character string (random seed) (see column 6, lines 45-54 and column 9, lines 62-67) and (see column 11, lines 3-29 and column 13, lines 13-26).

As per claim 25, Roberts discloses wherein the recipient is adapted to determine the hash key using the identification key (SPI) and the character string (random seed) and decrypt the encrypted data using the hash key (see column 6, lines 45-54 and column 9, lines 62-67) and (see column 11, lines 3-29 and column 13, lines 13-26).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter

sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 6, 9, 10, 13, 16-18, 20-21, and 26-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,931,128 to **Roberts** in view of US Patent 6,751,736 to **Bowman et al.**

As per claim 3, Roberts does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses generating a signature using the secret string (private key) and the data and transmitting the signature to the recipient (see column 7, lines 59-67). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by

Bowman et al it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 6, Bowman et al discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29). Therefore, claim 6 is rejected on the same rationale as the rejection of claim 3 above.

As per claim 9, Roberts substantially discloses determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31); decrypting the encrypted data using the hash key (see column 10, lines 13-31). **Roberts** does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses generating a first signature by the sender using the secret string (private key) and the data and transmitting the first signature to the recipient (see column 7, lines 59-67). **Bowman et al** further discloses the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and

the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 10, Roberts substantially discloses determining the private key (master secret) at the recipient using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 58-67); determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31); decrypting the encrypted data using the hash key (see column 10, lines 13-31). **Roberts** does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses generating a signature by the sender using

the secret string (private key) and the data and transmitting the signature to the recipient (see column 7, lines 59-67). **Bowman et al** further discloses determining the private key (secret sting) at the recipient using the identification key (secret ID) (see column 9, lines 27-29); determining the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); decrypting the encrypted data at the recipient using the hash key (see column 9, lines 33-35); and verifying the signature at the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 13, Bowman et al discloses wherein determining the private key comprises accessing a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29). Therefore, claim 13 is rejected on the same rationale as the rejection of claim 10 above.

As per claim 16, Bowman et al discloses receiving a signature from the sender (see column 7, lines 59-67); and verifying the signature using the decrypted data, the private key (secret sting), and the character string (random string) (see column 9, lines 29-55). Therefore, claim 16 is rejected on the same rationale as the rejection of claim 10 above.

As per claim 17, Bowman et al discloses receiving a signature from the sender (see column 7, lines 59-67), determining a hash key using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); and verifying the signature using the decrypted data and the hash key (see column 9, lines 29-55). Therefore, claim 17 is rejected on the same rationale as the rejection of claim 10 above.

As per claim 18, Roberts substantially discloses determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31). **Roberts** does not explicitly disclose generating a second signature using the hash key and the decrypted data and comparing the signatures. **Bowman et al** in an analogous art discloses receiving a first signature from the sender (see column 7, lines 59-67); determining

the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); generating a second signature by the sender using the secret string (private key) and the decrypted data (see column 9, lines 33-50); and comparing the first signature to the second signature (see column 9, lines 43-50). **Bowman et al** further discloses the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 20, Roberts does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses a signature engine (hash algorithm) stored in the memory and executable by the processor, (see column 13, lines 10-39) the signature engine adapted to generate a signature using the secret string (private key) and the data, the processor further adapted to transmit the signature to the recipient (see column 7, lines 59-67). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 21, Bowman et al discloses wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data (see, column 9, lines 33-55). Therefore, claim 21 is rejected on the same rationale as the rejection of claim 20 above.

As per claim 26, Bowman et al discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29). Therefore, claim 26 is rejected on the same rationale as the rejection of claim 20 above.

As per claim 27, Roberts substantially discloses a system for secure data transmission, (see fig. 11) comprising: a processor adapted to receive a plurality of encrypted data packets, an identification key (SPI), and a plurality of character strings (random seed) from a sender, each of the plurality of character strings correspond to one of the plurality of encrypted data packets (see column 11, lines 3-29 and column 13, lines 13-26); a memory coupled to the processor (see fig.1); a decryption engine stored in the memory and executable by the processor, the decryption engine adapted to decrypt the encrypted data packets using the respective character strings (random seed) and the private key (master secret) (see column 4, lines 8-23 and column 10, lines 13-31). **Roberts** does not explicitly disclose a relational database stored in the memory and accessible by the processor, the relational database relating the identification key to a private key. **Bowman et al** in an analogous art discloses a relational database stored in the memory and accessible by the processor, the relational database relating the identification key (secret ID) to a private key (secret sting) (see column 9, lines 27-29). Therefore, it would have been obvious to

one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a relational database because it would make it easier to select the corresponding private key to generate the encryption key as suggested by **Bowman et al** (see column 9, lines 27-29).

As per claim 28, the references as combined above disclose a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string (random seed) and a private key (master secret) and the decryption engine adapted to decrypt the encrypted data using the hash key (see **Roberts**, column 7, lines 32-67) and (see **Roberts**, column 11, lines 3-29 and column 13, lines 13-26). (See also **Bowman et al** column 9, lines 29-35)

As per claim 29, the references as combined above disclose comprising a signature engine (hash algorithm) stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the private key (secret sting), and the character string (random string) (see **Bowman et al** column 9, lines 29-55). Therefore, claim 29 is rejected on the same rationale as the rejection of claim 27 above.

As per claim 30, the references as combined above disclose a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key (secret sting), and the character string (random string) (see **Bowman et al** column 9, lines 29-55); and a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the

hash key and the decrypted data (see **Bowman et al** column 9, lines 29-55). Therefore, claim 30 is rejected on the same rationale as the rejection of claim 27 above.

As per claim 31, the references as combined above disclose a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string (random seed) with the private key (master secret) and the decryption engine adapted to decrypt the encrypted data using the hash key (see **Roberts**, column 7, lines 32-67) and (see **Roberts**, column 11, lines 3-29 and column 13, lines 13-26) (see **Bowman et al** column 9, lines 29-35).

As per claim 32, the references as combined above disclose a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (random seed) and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string (random seed) and the private key (master secret) (see **Roberts**, column 7, lines 12-32 and column 11, lines 3-29 and column 13, lines 13-26) (see **Bowman et al** column 7, lines 25-29; column 9, lines 29-55 and column 11, line 65 through column 12, line 14).

As per claim 33, the references as combined above disclose a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string; a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key; and wherein the

decryption engine is further adapted to encrypt data for transmitting to the sender using the hash key (see **Roberts**, column 7, lines 12-32 and column 11, lines 3-29 and column 13, lines 13-26) (see **Bowman et al** column 7, lines 25-29; column 9, lines 29-55 and column 11, line 65 through column 12, line 14).

As per claim 34, Bowman et al discloses a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a first signature using the decrypted data and compare the first signature to a second signature received from the sender (see column 9, lines 29-55). Therefore, claim 34 is rejected on the same rationale as the rejection of claim 27 above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see PTO-form 892).

5.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Examiner, Art Unit 2136
June 13, 2008